IN THE SPECIFICATION

Please replace the following paragraphs in the Specification with the following rewritten paragraphs:

[1000] This application claims priority to U.S. Provisional Application No. 60/452,358, filed on March 5, 2003, U.S. Provisional Application No. 60/452,914, filed on March 7, 2003 and U.S. Provisional Application No. 60/460,839, filed on April 5, 2003.

[1023] The word "exemplary" is used herein to mean "serving as an example, instance, or illustration." Any embodiment or design described herein as "exemplary" is not necessarily to be construed as preferred or advantageous over other embodiments or designs. Moreover, in the following description, "location" and "position" are synonymous terms that are used interchangeably.

[1029] Home network 210 includes various network entities that communicate with each other via an IP network 212. A network entity is a logical entity within a network and is designated to perform a particular function. Similarly, serving network 250 includes various network entities that communicate with each other via an IP network 252. IP networks 212 and 252 further couple to an Internet IP network 292. The network entities within home network 210, serving network 250, and third party network 290 may communicate with each other via IP networks 212, 252, and 292.

[1031] Within home network 210, LCS server 216 is a network entity designated to serve as a location server for location disclosure. LCS server 216 interacts with a home authentication, authorization, and accounting entity (H-AAA) 218 to perform authentication and authorization for location disclosure. A database 222 is used to store subscription information for subscribers (i.e., users) of home network 210. Each user is normally required to have a "subscription" for each wireless communication network to which access is desired. A subscription comprises pertinent information needed to access a designated wireless communication network, such as

subscriber/user identification information, security information, and so on. The subscription for each user is also referred to as a "subscriber profile" or a "user profile". The subscription information in database 222 may be updated by an LCS subscription manager 220 and accessed by H-AAA 218 for authentication, authorization, and accounting purposes. A message center 230 is responsible for storing, relaying, and forwarding SMS messages for mobile stations. A home location register (HLR) 224 stores registration information for mobile stations that have registered with home network 210.

[1033] Domain name system (DNS) servers 232 and 262 translate domain names (e.g., www.domain-name.com) into IP addresses (e.g., 204.62.131.129), which are required by network entities to communicate with each other via the IP networks. Each DNS server receives DNS queries from other network entities for IP addresses of domain names, determines the IP addresses for these domain names, and sends DNS responses with the IP addresses back to the requesting network entities. A DNS server in a given network (e.g., DNS server 232) may exchange information with other DNS servers in other networks (e.g., DNS server 262) to obtain the requested IP addresses.

[1045] Since location determination and location disclosure are treated as separate processes, different call flows may be defined and used for these two processes. A call flow is a sequence of steps that can be performed to achieve a given result. Each step in a call flow may invoke a particular procedure. Exemplary call flows are described below for (1) discovery of the IP address of SMPC 256 (for a roaming mobile station), (2) authentication, authorization, and session key setup, (3) mobile-originated location determination and location disclosure, (4) mobile-terminated location determination and location disclosure, and (5) other LCS related functions.

[1060] For call flow 450, mobile station 280 initially sends a *Location Disclosure Session Key Request* message to LCS server 216 (step 462). This message requests a new Session Key 2 for location disclosure and includes the NAI for mobile station

280. LCS server 216 then sends to H-AAA 218 a RADIUS *Access Request* packet (step 464). This packet contains an EAP message that further contains an EAP Response field with the NAI. H-AAA 218 runs the AKA procedures and generates a random number (RAND) and an authentication value (AUTN) (step 466). H-AAA 218 then responds by sending back a RADIUS *Access Response* packet (step 468). This packet contains an EAP message that further contains an EAP Request field. The EAP Request field carries an AKA Challenge that includes the AUTN and RAND generated by H-AAA 218. LCS server 216 receives the RADIUS *Access Response* packet from H-AAA 218 and forwards the EAP Request with the AKA Challenge (over UDP) to mobile station 280 (step 470).

[1061] Mobile station 280 receives the EAP Request from LCS server 216 , runs the AKA procedures, and verifies the received AUTN. If the received AUTN is checked, then mobile station 280 generates a new Session Key 2 and a RES based on the received RAND (step 472). Mobile station 280 then responds by sending to LCS server 216 an EAP Response with an AKA Response that includes the RES (step 474).

[1062] LCS server 216 then resubmits to H-AAA 218 its original RADIUS *Access Request* packet (step 476). This packet contains the AKA Response with the RES provided by mobile station 280. H-AAA 218 authenticates mobile station 280 based on the AKA Response. Upon successfully authenticating mobile station 280 by checking the RES, H-AAA 218 sends a RADIUS *Access Response* packet to LCS server 216 (step 478). This packet contains an EAP message that further contains an EAP Success field. The EAP Success field contains the user profile for mobile station 280, which is obtained from database 222. H-AAA 218 also return security information. The security information may include, for example, the Session Key 2, Session Key 2 RAND, and Session Key 2 lifetime.

[1063] LCS server 216 receives the RADIUS *Access Response* packet from H-AAA 218 and may retain the user profile and the Session Key 2 for its own use. LCS server 216 then sends the EAP Success (over UDP) to mobile station 280 (step 480).

LCS server 216 next authorizes mobile station 280 by checking the user profile (step 482). LCS server 216 then sends to mobile station 280 a *Location Disclosure Session Key Response* message that includes the Session Key 2 lifetime (step 484).

[1065] Call flow 400 shows the use of the MD-5 algorithm for location determination, and call flow 450 shows the use of the AKA procedures for location disclosure. Other security algorithms may also be used for location determination and location disclosure, and this is within the scope of the invention. For example, a CAVE (Cellular Authentication and Voice Encryption) algorithm may be used for access authentication. A CHAP (Challenge Handshake Authentication Protocol) and a Mobile IP Protocol may be used for IP authentication. The CAVE, CHAP, and Mobile IP algorithms are well known in the art.

[1076] If authentication and authorization does not need to be performed, then steps 516, 518, and 520 are skipped. Otherwise, call flow 400 in FIG. 4A is performed and SMPC 256 may or may not receive a new Session Key 1, a new Session Key 1 RAND, and a new Session Key 1 lifetime from H-AAA 218 (step 516). If SMPC 256 does not receive a new Session Key 1 from H-AAA 218 from performing step 516, then steps 518 and 520 are skipped. If SMPC 256 receives a new Session Key 1 from H-AAA 218 from performing step 516, then SMPC 256 sends to SPDE 260 a GEOPOSREQ message that includes this Session Key 1 (step 518). SPDE 260 then responds by sending a geoposreq message back to SMPC 256 (step 520). The GEOPOSREQ and geoposreq messages are described in TIA/EIA/PN-4747. Step 516 may or may not be performed for call flow 500, and this is indicated by a dashed box around step 516. Steps 518 and 520 may or may not be performed, and this is also indicated by a dashed box around steps 518 and 520.

[1081] For call flow 550, mobile station 280 initiates a data call to set up a PPP session with PDSN 270 (step 552). Mobile station 280 then sends to SMPC 256 a Mobile Originated Positioning Request message that includes the NAI for mobile station 280 (step 554). SMPC 256 next determines the ID of the serving cell with which mobile station 280 currently communicates. SMPC 256 then sends to SPDE

260 a GEOPOSREQ message with an indication that the cell-ID method is being used (step 556). SPDE 260 receives this message from SMPC 256 and sends back a geoposreq message that includes location information for mobile station 280. This location information may include a location estimate for the mobile station (based on the serving cell ID), the location accuracy or uncertainty, and so on.

[1096] For call flow 700, LCS server 216 sends an SMS *Delivery Point-to-Point Invoke* (SMDPP) message to message center 222, which serves mobile station 280 (step 712). This SMDPP message includes a Push Notification and the IMSI of mobile station 280. The Push Notification is used to invoke mobile station 280 to initiate a data call so that its IP address may be set up. The IMSI (International Mobile Subscriber Identification) is a number that can uniquely identify mobile station 280. Upon sending the SMDPP message, LCS server 216 starts a timer, which is used to time-out the wait for a reply for the SMDPP message. Message center 230 receives the SMDPP message from LCS server 216 and sends back an smdpp return result (step 714).

[1097] Message center 230 needs to know the SMS address of the current serving network for mobile station 280. The SMS address is used to send SMS messages to mobile station 280. Message center 230 then sends an *SMS Request Invoke* (SMSREQ) message to HLR 224 (step 716). If HLR 224 has the SMS address of serving network 250 (which is the current serving network for mobile station 280), then HLR 224 replies with an smsreq message that contains this SMS address (step 718). Otherwise, HLR 224 forwards the SMSREQ message toward serving network 250 (not shown in FIG. 7).

[1098] Upon receiving the SMS address of serving network 250, message center 230 sends the SMDPP message to MSC 272 in serving network 250 (step 720). The SMDPP message is sent using the SMS address obtained from HLR 224 or serving network 250 in step 718. MSC 272 receives the SMDPP message from message center 230 and pages mobile station 280. MSC 272 also extracts the Push Notification from the received SMDPP message, includes the Push Notification in an

SMS Delivery Request (SMD-REQ) message, and sends the SMD-REQ message over the air to mobile station 280 (step 722). Mobile station 280 receives the SMD-REQ message and replies with an *SMS Delivery Acknowledge* (SMD-ACK) message (step 724). MSC 272 receives the SMD-ACK message from mobile station 280 and returns an smdpp message to message center 230 (step 726).

[1103] **FIG. 8B** shows an exemplary call flow 850 for performing mobile-terminated location determination with the cell-ID method. Call flow 850 includes steps 856, 858, 860, and 862, which correspond to steps 556, 558, 560, and 562, respectively, in call flow 550 in FIG. 5B. Steps 552 and 554 are omitted from call flow 850. Moreover, a *Mobile Terminated Positioning Request* message is used for step 860 whereas a *Mobile Originated Positioning Response* message is used for step 560

[1107] The user profile for mobile station 280 may indicate that user verification is needed prior to each disclosure of the location information for mobile station 280. In this case, LCS server 216 and mobile station 280 perform mutual authentication using call flow 450 in FIG. 4B (step 914). LCS server 216 then sends a *User Verification Request* message (which may be signed and/or encrypted using the Session Key 2 obtained in step 914) to mobile station 280. Mobile station 280 responds by sending back a *User Verification Response* message (which may also be signed and/or encrypted using the Session Key 2 obtained in step 914). This message indicates that disclosure of the location information for mobile station 280 is allowed. Since steps 914, 916, and 918 may or may not be performed for call flow 900, depending on the user profile, these steps are surrounded by dashed boxes. LCS server 216 then sends to LCS provider 202x a *Location Service Response* message that includes the location information for mobile station 280 (step 920).

[1116] Accounting and billing may be performed in LCS server 216 within home network 210 and/or SMPC 256 within serving network 250. SMPC 256 may generate a call detail record (CDR) for each location determination request. Correspondingly, LCS server 216 may generate a CDR for each location disclosure

request. The CDRs may be used for accounting, billing, and/or other purposes. Table 4 lists various items that may be included in a CDR.